REMARKS

In view of the following discussion, the Applicants submit that all of the claims now pending in the application fully satisfy the requirements of 35 U.S.C. §112, 35 U.S.C. §102, and 35 U.S.C. §103. Thus, the Applicants believe that all of these claims are now in allowable form.

I. REJECTION OF CLAIMS 1-17 UNDER 35 U.S.C. § 112

The Examiner rejected claims 1-17 under 35 U.S.C. § 112, second paragraph, for allegedly omitting essential elements. In response, the Applicants have amended independent claim 1, from which claims 2-17 depend, in order to more clearly recite aspects of the invention.

In particular, independent claim 1 has been amended, in accordance with the Examiner's suggestion, to specify that a particular configuration of the new server configuration for the first server depends on the total number of times that the first server has been victim of a security assault or a possible security assault.

In light of this amendment, the Applicants respectfully submit that independent claim 1 fully satisfies the requirements of 35 U.S.C. § 112. Moreover, claims 2-17 depend from independent claim 1 and incorporate at least all of the features of independent claim 1. As such, and for the same reasons stated above with respect to independent claim 1, the Applicants respectfully submit that claims 2-17 also fully satisfy the requirements of 35 U.S.C. § 112. Accordingly, the Applicants respectfully request that the rejection of claims 1-17 under 35 U.S.C. § 112 be withdrawn.

II. REJECTION OF CLAIMS 1-11 AND 13-17 UNDER 35 U.S.C. § 102

The Examiner rejected claims 1-11 and 13-17 as being anticipated by the Smithson et al. patent (U.S. Patent No. 6,898,715, issued May 24, 2005, hereinafter referred to as "Smithson"). The Applicants respectfully traverse the rejection.

In particular, the Examiner's attention is respectfully directed to the fact that Smithson fails to disclose or suggest incrementing a counter that tracks a total number of times that a server has been victim of a security assault and automatically creating a new server instance with a new server configuration if the value of the counter does not exceed a maximum limit, where the new server configuration is selected from a table comprising a plurality of new server configurations, such that the particular configuration of the new server configuration depends on the total number of times that the server has been victim of a security assault (*i.e.*, as indicated by the value of the counter), as recited in independent claim 1.

By contrast, Smithson teaches the execution of a predefined series of steps in response to a virus outbreak detected on a computer. Specifically, Smithson teaches that these predefined steps are executed in a particular order and gradually escalate until it is determined that "the virus outbreak has been overcome" (Smithson, column 5, line 66 – column 6, line 3). The Examiner suggests in the Office Action that this is equivalent to a counter that tracks the number of times that a server has been the victim of a security assault, because "it is inherent in the predefined sequence that there would be a counter to keep track of which step will be processed next" (Final Office Action, Page 3). Even accepting the Examiner's suggestion that the counter would be inherent in Smithson's teachings, however, this counter still does not track the number of times that the computer has been the victim of a security assault (*e.g.*, the number of viruses to which the computer has fallen victim). As the Examiner correctly points out, such a counter would, at best, track which step in the predefined series of steps to execute next. These steps do not correspond to the total number of times that the computer has been assaulted, as claimed by the Applicants in independent claim 1, but rather correspond to the severity of a single assault (in that each step is executed only if the previous step failed to overcome the virus).

Thus, additionally, Smithson also fails to teach or suggest that the particular configuration of a new server configuration is dependent upon the total number of times that the server has been the victim of a security assault, as also claimed by the Applicants in independent claim 1. At best, a new configuration of the computer according to Smithson would be the result of the execution of one or more of the predefined series of steps, as suggested by the Examiner ("each execution of a step is considered by examiner to be a new server instance ...," Final Office Action, Page 3). Thus, at best, the new configuration of the computer would be dependent upon the severity of a single assault (*i.e.*, how many steps in the predefined series were necessary to overcome the virus).

Thus, Smithson fails to teach or suggest every limitation of the Applicants' independent claim 1. Specifically, independent claim 1 recites:

> 1. A method for automated adaptive reprovisioning of servers under security assault, the method comprising:
>
> detecting a security assault or a possible security assault on a first server;
> incrementing a counter that tracks a total number of times that the first server has been victim of a security assault or a possible security assault;
> notifying a human operator if a value of said counter exceeds a maximum limit;
> and
> reprovisioning by automatically creating a new server instance with a new server configuration to perform at least one of the tasks performed by said first server, if said value of said counter does not exceed the maximum limit, wherein said new server configuration for said new server instance is selected from a table comprising a plurality of new server configurations, said new server configuration being associated in said table with said value of said counter such that a particular configuration of said new server configuration depends on the total number of times that said first server has been victim of a security assault. (Emphasis added)

Applicants' invention is directed to a method and apparatus for adaptive server reprovisioning under security assault. When an assault on a server is detected, the server may be reconfigured in accordance with one of a number of potential new configurations designed to improve the server's resistance to subsequent assaults. These potential new configurations are stored in a table. Embodiments of the invention track (via a counter) a number of times that the server has been assaulted and use this number as an index into the table of potential new configurations, where at least one of the potential new configurations will correspond, according to the table, to the number of times that the given server has been assaulted. If the number of times that the server has been assaulted exceeds a predefined maximum number, a human operator is notified instead. In this way, a new configuration for the server can be selected automatically, based on the server's recorded vulnerability, and in a manner that minimizes server downtime and human intervention.

Applicants' independent claim 1 clearly recites the steps of incrementing a counter that tracks a total number of times that a first server has been victim of a security assault and automatically creating a new server instance with a new server configuration if the value of the counter does not exceed a maximum limit, where the new server configuration is selected from a table comprising a plurality of new server configurations, each of which is associated in the table with the value of the counter, such that a particular configuration of said new server configuration depends on the total number of times that the server has been victim of a security assault. As discussed above, Smithson fails to teach or suggest these features. Accordingly, the Applicants respectfully submit that independent claim 1 is not anticipated by Smithson and is patentable under 35 U.S.C. §102.

Claims 2-11 and 13-17 depend from independent claim 1 and incorporate at least all of the features of independent claim 1. As such, and at least for the same reasons set forth with respect to independent claim 1, the Applicants respectfully submit that claims 2-11 and 13-17 are also not anticipated by Smithson and are patentable under 35 U.S.C. §102. Accordingly the Applicants respectfully request that the rejection of claims 2-11 and 13-17 under 35 U.S.C. §103 be withdrawn.

III. REJECTION OF CLAIM 12 UNDER 35 U.S.C. § 103

The Examiner rejected claim 12 as being unpatentable over Smithson. The Applicants respectfully traverse the rejection.

As discussed above, Smithson fails to teach or suggest the steps of incrementing a counter that tracks a total number of times that a first server has been victim of a security assault and automatically creating a new server instance with a new server configuration if the value of the counter does not exceed a maximum limit, where the new server configuration is selected from a table comprising a plurality of new server configurations, each of which is associated in the table with the value of the counter, such that a particular configuration of said new server configuration depends on the total number of times that the server has been victim of a security assault, as recited by the Applicants in independent claim 1. Accordingly, the Applicants respectfully submit that independent claim 1 is not made obvious by Smithson and is patentable under 35 U.S.C. §103.

Claim 12 depends from independent claim 1 and incorporates at least all of the features of independent claim 1. As such, and at least for the same reasons set forth with respect to independent claim 1, the Applicants respectfully submit that claim 12 is also not made obvious by Smithson and is patentable under 35 U.S.C. §103. Accordingly the Applicants respectfully request that the rejection of claim 12 under 35 U.S.C. §103 be withdrawn.

IV. CONCLUSION

Thus, the Applicants submit that all of the presented claims fully satisfy the requirements of 35 U.S.C. §112, 35 U.S.C. §102, and 35 U.S.C. §103. Consequently, the Applicants believe that all these claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

If, however, the Examiner believes that there are any unresolved issues requiring the maintenance of the final action in any of the claims now pending in the application, it is requested that the Examiner telephone Kin-Wah Tong, Esq. at (732) 842-8110 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Respectfully submitted,

April 27, 2009

Wall & Tong, LLP
595 Shrewsbury Avenue
Shrewsbury, New Jersey 07702

Kin-Wah Tong, Attorney
Reg. No. 39,400
(732) 842-8110